DOI: 10.53477/2971-8813-22-56

CYBER DOCTRINARY APPROACHES CASE STUDY – FRENCH REPUBLIC, FEDERAL REPUBLIC OF GERMANY AND THE KINGDOM OF SPAIN

Lucian-Alexandru ENE
Officer, Ministry of National Defense
enelual@gmail.com

Abstract: *In this paper, we aim to highlight the national efforts that representative countries of the European Union (EU) have made to harmonize national goals, with those of the NATO, in the field of cybernetics. This study also focuses exclusively on the approach of the French Republic, the Federal Republic of Germany and the Kingdom of Spain, in the field of cyber defense developments, while analyzing evolutionary concepts and phases in the field, at Allied and European levels.*

Keywords: *the French Republic; the Federal Republic of Germany; the Kingdom of Spain.*

Introduction

The entry into the third year of the Covid-19 Pandemic, finds the world facing the goal of "learning to live with the SARS CoV-2 virus". Global health crisis management (COVID-19) is affected by the difficulty of reaching the vaccine in poor countries, as well as completely unbalanced vaccination rates between underdeveloped and rich countries.

The economic recovery forecast for 2022 is under the auspices of the global energy crisis, logistical bottlenecks and increasingly difficult financial lending conditions.

The transition from a world centered on US influence and US geopolitical and geostrategic lines to one marked by the economic influence of the People's Republic of China (PRC) is increasingly present. Also, the aspirations of reaffirmation as an actor with global influence manifested by the military pressures of the Russian Federation especially in Ukraine, but also in Kazakhstan, Syria, Mali (Africa), the Republic of Moldova, Belarus make that, the planet, in 2022, to be a land of extreme challenges. But, as we all know, any crisis, be it of an economic, security, health, or political nature, together with the characteristic elements of instability and uncertainty, paves the way for multidimensional aspects of opportunity (economic, security, etc.) from which it can benefit those (actor/actors) who manage (quickly and completely) to identify opportunities and manage them in their favor.

Contextual delimitations – 2022

Also, the Huygensian waves of the political and economic "earthquakes" of 2021, such as: political-security tensions between Washington and Beijing, the Kremlin's strategic politico-military game in Ukraine, redefining EU-US and EU-UK relations, the emergence of the AUKUS agreement, the rapid and debatable withdrawal of allied troops from Afghanistan, the redefinition of the foreign policy lines of Turkey, India, Australia and Brazil, the harmonization of strategic interests between the Chinese PR and FRUS, are part of the hypothesis of the security equation of the beginning of 2022.

Characteristic of any equation with many variables and unknowns the solutions can be multiple, and the way to solve it (equation) depends on the "established formulas" applied, the degree of complexity of the proposed situation to solve, but especially the will, skill, experience and at the same time the interests, the person in charge, the person, entity, organization, or state actor in “finding” the solutions.

We cannot say that the global security environment, at the beginning of 2022, differs radically from previous years, but it is unanimously accepted that the degree of security instability is following an increasing trend, which peaked on February 24 (date at which the Russian Federation invaded Ukraine).

The war in Ukraine and the lessons learned from this tragedy, as well as the technological evolution and transformation of the battlefields, call for a profound change in military thinking at the strategic level.

Thus, politico-military strategies are called to reconceptualize the planning of military actions, simultaneously and integrated, in all new areas - land, air, sea, space and cybernetics (https://formiche.net/2022/01/all-domain-presentazione-airpress/ n.d.).

In this paper, we aim to highlight the national efforts that representative countries of the European Union (EU)[1] have made to harmonize national provisions, with those of the North Atlantic Treaty Organization (NATO), in the field of cybernetics. This study also focuses exclusively on the approach of the French Republic (France), the Federal Republic of Germany (Germany) and the Kingdom of Spain (Spain) in the field of cyber defense development, while analyzing evolutionary concepts and phases in this fields, at Allied and European levels.

NATO Allied Cyber Approaches

Regarding NATO's cyber defense approach, it can be said that in the last 20 years, the field has received significant attention and developments.

The cyber domain first appeared on the agenda of the NATO talks at the Prague Summit (2002), and later, at the Riga Summit (2006), cyber defense was confirmed as priority for the politico-military alliance. In 2008, in Bucharest, during the Summit of Heads of State and Government, the first Cyber Defense Policy was approved[2], and in 2010, in the context of the Lisbon Summit, because of the intensification of cyber-attacks and the rapid evolution due to their complexity, the NATO Strategic Concept states that cyber threats can affect the security of vital national infrastructures and also the stability of the Euro-Atlantic (nato.mae.ro n.d.).

At the 2014 Summit in Wales, improvements were made to NATO's Cyber Defense Policy and at the same time agreed on the opportunity to extend the application of the solidarity clause in Article 5 of the North Atlantic Treaty to cyber (www.analisidifesa.it n.d.).

Two years later, at the Warsaw Summit, member states reaffirmed NATO's purely defensive mission in cyberspace[3] and at the same time declared cyberspace an operational domain (www.nato.int n.d.).

Following these political decisions, the first concrete step of the Alliance was the establishment, in 2018, of the Center of Excellence for Cyber Defense (CCDCOE), a NATO affiliate[4], based in Estonia (Tallinn). The centre's mission is to provide NATO member states

[1] EU member countries and members of the North Atlantic Treaty Organization

[2] The Bucharest Summit not only formalized NATO's first cyber defense policy, but also laid the groundwork for an allied cyber protection ecosystem designed to strengthen existing defense capabilities and facilitate development.

[3] It was agreed to strengthen and improve, as a matter of priority, the cyber defense of national networks and infrastructures. It was also acknowledged that the continued adaptation of national and NATO cyber defense capabilities will strengthen the Alliance's cyber defense and overall resilience.

[4] CCDCOE is staffed and funded by the Republic of Austria, the Kingdom of Belgium, the Republic of Bulgaria, Canada, the Republic of Croatia, the Czech Republic, the Kingdom of Denmark, the Republic of Estonia, the Republic of Finland, France, Germany, the Hellenic Republic, Hungary, Ireland, the Italian Republic, Japan, Republic of Latvia, Republic of Lithuania, Grand Duchy of Luxembourg, Montenegro, Kingdom of the Netherlands, Kingdom of Norway, Republic of Poland, Portuguese Republic, Romania, Slovak Republic,

with interdisciplinary expertise in cyber defense research, training, and exercises (cdcoe.org n.d.). Romania officially joined the CCDCOE on June 13, 2019 (www.mae.ro n.d.), and in the same year, NATO drafted the Guide to Strengthen the Alliance's Response to Cyber Activities, which includes a set of tools for responding to malicious, significant cyber activities (www.nato.int, www.nato.int n.d.).

With regard to bilateral cooperation between NATO and the EU, in the Joint NATO-EU Declaration (2016), the cyber domain is presented as a priority, focusing on the specific dimensions of cyber security and defense, including in the context of missions, operations, exercises and joint trainings (European Commission and the Secretary General of the North Atlantic Treaty Organization n.d.). Also, in 2016[5], NATO and the EU signed a Technical Agreement in the field of Cyber Defense regulating the methodology for conducting the exchange of cyber information between the EU IT Emergency Response Team (CERT-EU) and NATO Computer Incident Response Capability (NCIRC) (EU CYBER DEFENSE POLICY (FRAMEWORK n.d.).

Also, the bilateral cooperation between the two organizations in the field of cyber defense is continuously developed by holding regular meetings, both at the level of politico-military decision makers, and especially at the level of experts.

The national approach of the French Republic

The field of cyber defense enjoys a special focus on the responsible factors in the field in France. On 12 February 2018, under the coordination of the General Secretariat for Defense and Security (Le Secretariat Général de la Défense et de la Sécurité National Strategy for Combating Cyber Threats (Revue Strategic cyber defense)(General Secretariat for Defense and Security Strategy of France). Within the Strategy, the 4 threats to which French cyber defense structures must respond are: computer espionage, cybercrime, institutional destabilization and cyber sabotage[6].

According to the document in use, computer espionage (computer science) is characteristic of developed intelligence services, which have designed and adapted their communications interception systems for economic, technological or political purposes.

Thus, computer espionage is only a transposition of traditional information activities (collection, processing, dissemination) in the digital world. This activity is not exclusively the prerogative of the intelligence services assigned to some state actors, but can also be carried out by elements, individual or organizational, with non-state organizational correspondence.

At the end of the last century, cybercrime was perceived as a combination of specialized actions of isolated persons with technical skills (hackers), without a political or financial motivation, carried out to fulfill an "individual" purpose[7]. The emergence of BITCOIN[8] and virtual currencies, associated with the idea of "anonymizing" the concept, created the premises for the emergence of cybercrime, based on financial motivation.

Currently, cybercriminals, using basic methods, are able to get large sums of money. Direct theft of information considered sensitive or important, or money, using the Internet, from companies' computer networks[9] or their accounts[10], is considered the most common

Republic of Slovenia, Republic of Korea, Spain, Kingdom of Sweden, Swiss Confederation, Republic of Turkey, Kingdom United Kingdom of Great Britain and Northern Ireland and the United States of America.

[5] Modified in 2028, by EU CYBER DEFENSE POLICY FRAMEWORK.

[6] *Ibidem*, p.11.

[7] *Ibidem*, p.12.

[8] The first Bitcoin transaction for a good appeared on May 21, 2010, when a Bitcoin user named Laszlo bought a $ 25 pizza worth 10,000 Bitcoin, https://bitcoinromania.ro/blog/istoria-bitcoin/, accessed on 30.04.2022.

[9] Exfiltration and then resale of information.

[10] In case of fraudulent money transfers.

method used by cybercriminals. The second, ex-filtering the information and then recontacting the injured party for redemption, involves time and associated risks.

The strategy to combat cyber threats underlies the drafting of the White Paper on Combating Cyber Threat, a document with inter-ministerial responsibilities that projects a clear picture of the French national cyber risk and outlines the actions needed to strengthen the country's technological infrastructure of the capacities to respond to a possible cyber-attack, to the address of the institutional security – cyber[11].

At the same time, the White Paper on Defense laid the foundations for the establishment of the National Agency for the Management of Cyber Attacks and the Protection of the State Information System (www.legifrance.gouv.fr n.d.), which allowed for better cyber coordination at the inter-ministerial level (www.penseemiliterre.fr/ n.d.).

Thus, in case of a hostile cyber incident affecting the security of the state (www.senat.fr) the Cyber Crisis Coordination Center (C4) which brings together the responsible ministries (www.liberation.fr/france/ 2020) will provide decision-making power, the Ministry of Defense, which will act through the Cyber Defense Command (Comcyber – established in 2017).

Subsequently, as a result of the development of new technologies, but especially due to the increase in the number of cyber-attacks suffered by the Ministry of Defense, under the Military Planning Law (2019-2025 – Programming Law Militaire, Lpm) proposed: making investments in the cyber field, worth 1.6 billion euros and increasing the specialized staff by approx. 1000 people (to be distributed within the structures of Comcyber, Directorate-General for External Security) general security extérieure (DGSE)) and within the General Emergency Directorate (Direction general alarm system (DGA)), so that by 2025 a total of 4500 specialists will be reached, half of whom will provide protection to information systems, a quarter of the staff will be dedicated to cyber defense and the rest will be specialized for actions cyber offensive (www.ifri.org n.d.). Of the planned budget allocation, € 200 million will be invested in the construction of a training center – cyber experts (Temple de la cyber defenses) in Saint-Jacques de la Lande.

French Defense Minister, Florence Parly, reiterated that France would not hesitate to use the cyber weapon in military operations and that operators in the sector would enjoy the same protections and rights as soldiers engaged in operations abroad in the performance of their duties.

In terms of Allied engagement, France supports the 2018 NATO Strategy, and stressed the importance of increasing Allied engagement and integrating cyber defense capabilities (www.cicde.defense.gouv.fr n.d.) into NATO operational scenarios and missions (www.sgdsn.gouv.fr 2018).

Conceptualization of the field (cyber) in the Federal Republic of Germany

In 2011, the National Cyber Security Council was established in Berlin, which includes representatives from various ministries (Ministry of the Interior, Foreign Affairs, Defense, Justice, Economic and Energy Affairs and Consumer Protection, Education and Research, Finance, Transportation and digital infrastructure, as well as private sector representatives), in order to propose the necessary updates for the new National Cyber Strategy (www.enisa.europa.eu n.d.).

Also in 2016, the Federal Republic of Germany updated its Cyber Security Strategy (the drafting of the programmatic document was initiated in 2011) using an inter-ministerial approach[12], which provides for action by both the federal government and the Länder/regions.

[11] *Ibidem,* p. 137.
[12] *Idem.*

In the programmatic document, special attention is paid to the need to have a National Cyber Response Center that provides a coordinated and integrated response and within the limits of relevant national and international legislation in the field.

Another element of novelty, introduced in 2016 (with the revision of the Strategy) is the provision on the ability to conduct cyber offensive operations in response to an attack. The Military Counterintelligence Service is responsible for managing responses to malicious, organized, and cyber events. The contribution of the Armed Forces is also foreseen (part regulated by the German Constitution and at the same time by the international legislation in the field). This fact is also mentioned in the White Paper on Defense (published, 2016)(www.researchgate.net) and which provides for a link between the cyber defense capabilities of the Armed Forces and the response capabilities of civilian cyber security structures, indicating the former as complementary in shaping the national cyber security architecture (although they are managed in separately).

Germany is involved in a process of consolidating previously developed infrastructure at the Army level. The purpose of developing response capabilities is to successfully create a single structure, consisting of military operational units[13], that is prepared, as equipment upgrades, to use in the future, artificial intelligence and other methods of big-data analysis, to formulate answer hypotheses as complete and complex as possible[14].

From a military point of view, the German Armed Forces have limited responsibilities and possibilities for action and/or collaboration with other state bodies, due to constitutional limitations, which clearly delimit the responsibilities of the Armed Forces in carrying out operations defined as "administrative assistance"[15].

In the case of an external cyber-attack, the extent of which requires the involvement of the Armed Forces[16], they must obtain parliamentary approval (which could take too long in the event of a rapid cyber-attack). However, in the context of the conduct of domestic cyber defense operations, the approval of the Bundestag is sufficient to allow the use of the cyber defense capabilities of the Armed Forces.

According to the White Paper on Defense, Berlin has created the Computer and Cyberspace Command, which is responsible for conducting network operations.

The structure provides for approximately 14,000 specialists to ensure a full operational capacity, planned to have been achieved by 2021 (www.difesaonline.it).

Given the fact that it is not always possible to define the perpetrator of a cyber-attack from the outset and considering the need to coordinate the various authorities involved for a coordinated and integrated response (www.researchgate.net), the Federal Government has set up the National Cyber Defense Center coordination of the various crisis response entities[17].

At national and international level, Germany emphasized the need for the most comprehensive regulatory framework and the establishment of partnerships and cooperation plans to achieve high levels of security and operational readiness, even in the event of a response to complex cyber-attacks[18]. At present, active defense operations are not explicitly regulated from a legal point of view, which is why there is a national debate on the appropriateness of providing hack - back actions (www.deutschlandfunk.de).

[13] https://doi.org/10.11610/Connections.19.1.02, p. 25, accessed on 01.05.2022.
[14] https://doi.org/10.11610/Connections.19.1.02, accessed on 01.05.2022.
[15] https://doi.org/10.1007/978-3-319-90014-8_4, p. 36, accessed on 01.05.2022.
[16] For the use of the Bundeswehr in the national territory, the attack must be carried out by a state actor.
[17] *Ibidem,* p.39.
[18] *Ibidem,* p.21.

Cyber domain in the Kingdom of Spain

In a top of the number of cyber-attacks directed against some member states of the European Union, Spain occupies an undesirable place, the leader in the ranking (www.enigmasoftware.com). Although some cyberattacks are targeted at sectors considered strategically irrelevant, others have serious implications, such as the one against 2019, directed against the Spanish Ministry of Defense, which sought to take over sensitive information from the defense industry (elpais.com/politica).

Thus, Spain's National Cyber Security Strategy was updated in 2019 (www.ccn.cni.es) to include the new provisions of the National Security Strategy, developed in 2017. Also in Spain, the Covid-19 Pandemic, brought into attention the necessity to update the strategic document, for to prevent the possible consequences of the cyber domain because of the global health crisis.

Royal Decree no. 521/2020 (www.boe.es) on the basic organization of the Armed Forces emphasizes the need for trained personnel and the existence of adequate structures/facilities and defense systems and advanced technology to enable the digitization of the Spanish Army, considering the growing trend of cyber threats.

Cyber defense is part of the broader field of cyber security which includes but is not limited to activities related to the Armed Forces. In order to implement this, Spain has set up an Emergency Response Team which is responsible for formulating a rapid response to cyber-attacks against citizens, businesses and other interest groups and an Emergency Response Team which is focused on responding to attacks on government institutions (cybernews.com).

Regarding the management of the situation at the level of the Spanish Armed Forces, the Joint Cyber Defense Command, a structure directly subordinated to the General Staff of the Spanish Defense, is the military organization responsible for conducting cyber defense actions, IT infrastructures within the Armed Forces. This Joint Command established seeks to implement the necessary actions to ensure the integrity of Spanish military capabilities.

The command (Legislative Collection of the Ministry of Defense 2013) is also the structure responsible for managing an appropriate response in the event of a cyber-attack at the national level.

The Spanish Ministry of Defense also has an emergency response team in the military sector, which is cooperating with other civilian structures. The structure has OPCOM at the head of defense and thus, cyber operations, more or less defensive, are integrated into the chain of command even in the situation of participation of the armed forces in a multinational context, either under the auspices of the UN, NATO or EU.

In this context, in the absence of a declared armed confrontation, there is currently no provision for the possibility of conducting cyber-offensive operations (Center Superior de Estudios de la Defensa Nacional 2012).

Conclusions

In the last twenty years, the number of cyber-attacks is constantly increasing, and the cyber threat is shaping up to represent a real threat to the defense of the rule of law. In order to limit the undesirable effects of the realization of the cyber threat, at the international level, multiple cooperation plans are being developed that aim at the legal regulation of the cyber domain. However, the results obtained are limited, the main cause being the differences in the conceptualization and approach of cyberspace, in particular, by certain international actors.

The issue of achieving a standardization of the field is amplified by 2 other variables. First of all, the difficulty of identifying the affiliation of a cyber-attack in the hypothetical situation in which there is an attack is committed, concentrated, by state actors, terrorist

groups, thus constituting an aggressor group difficult to define. Secondly, massive investments and the creation of standardized normative elements are needed to create specialized threat response capabilities (highly specialized technical staff, standardized regulations, intervention procedures, etc.).

The declaration of cyberspace as an operational domain has led to a significant qualitative leap in the approach to cyber threats at the Allied level. The conflict in Ukraine is increasingly debating the types of attacks that could trigger the collective defense clause in accordance with Article 5 of the North Atlantic Treaty. We also notice that the cyber domain has quickly become an integral part of both unconventional and conventional conflicts.

The analysis carried out at the level of the 3 European states, led to the identification of different approaches to the way of achieving cyber defense, which demonstrates the need to continue the idea of standardization and harmonization of national doctrines and procedures in the field. Thus, we noticed that within the programmatic documents of the analyzed states there are substantial differences in terms of the possibility and manner of carrying out both defensive actions and especially in terms of ability and legality to carry out offensive operations.

Thus, Germany and Spain are among the countries that believe that cyber deterrence can also be achieved through the state's ability to respond in a timely and proportionate manner to a cyber-attack, by assuming operations defined as hack -back.

On the other hand, Paris has a different understanding of the possibilities that arise from the active use of cyber defense. Thus, cyber defense and deterrence are equivalent to ensuring the ability to respond to cyber, but also to the possibility of active prevention against possible adversaries, consisting of either state actors or terrorist groups or organizations.

The analysis performed may indicate, a series of common needs and recommendations, at the Allied level and possible guidance that Romanian specialists can consider at the national level, as follows:

- the imperiousness of having a unitary doctrinal framework at the allied level.
- the existence of a better integration of the cyber domain within the allied command structures, which is also valid at national level.
- stepping up cooperation between research-focused private companies and government institutions.
- increase investment for up-continuous upgrading of existing cyber capabilities at allied and/or national level.
- intensification of training programs for specialized military personnel working in the field of cyber operations.
- and last but not least, the awareness of state officials, but also of the population regarding the threats in cyberspace and the possible future implications.

Bibliography

https://formiche.net/2022/01/all-domain-presentazione-airpress/
https://nato.mae.ro/node/435
https://www.analisidifesa.it/2019/06/come-cambia-la-strategia-cyber-della-nato/
https://www.nato.int/cps/en/natohq/official_texts_133177.htm
https://ccdcoe.org/about-us/
https://www.mae.ro/node/5337
https://www.nato.int/cps/en/natohq/topics_78170.htm
https://www.consilium.europa.eu/media/21481/nato-eu-declaration- 8- iulie-en-final.pdf
https://www.consilium.europa.eu/media/37024/st14413-en18.pdf
http://www.sgdsn.gouv.fr/uploads/2018/02/20180206-np-revue-cyber-public-v3.3 publication.pdf

https://bitcoinromania.ro/blog/istoria-bitcoin/
https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000020828212/
https://www.penseemiliterre.fr/ressources/30147/14/la_strategie_francaise_de_cyberdefense.pdf
http://www.senat.fr/rap/r19506/r1950638.html#:~:text=b)%20Le%20centre%20de%20coordination% 20des% 20crises% 20cyber% 20 (C4) & tex = Il% 20est% 20un% 20m% C3% A9canisme% 20permanent, minist% C3% A8res% 20concern% C3% A9s% 20par% 20la%
https://www.liberation.fr/france/2020/01 / 30 / cyber-a-la-francaise-l-attaque-et-la-defense-de-la-separation-al-interaction_1776147
https://www.ifri.org/sites/default/files/atoms/files/044_051_cyberguerre-2.pdf
https://www.cicde.defense.gouv.fr/images/documentation/architectures/20190805_DOM320.pdf
https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/national-cyber-security-strategies-interactive-map/ strategies / cyber-security -strategy-for-germany / @@ download_version / 5f3c65fe954c4d33ad6a9242cd5bb448 / file_en .
https://www.researchgate.net/publication/326511119_The_Evolution_of_German_Cybersecurity_Strategy
https://doi.org/10.11610/Connections.19.1.02
https://doi.org/10.11610/Connections.19.1.02
https://doi.org/10.1007/978-3-319-90014-8_4
https://www.difesaonline.it/evidenza/cyber/anche-la-germania-ha-la-sua-quarta- armed forces
https://www.deutschlandfunk.de/aktive-cyber-abwehr-fuer-deutschland-der-geheime-krieg-im.724.de.html?dram:article_id= 461140
https://elpais.com/politica/2019/03/25/actualidad/1553543912_758690.html
https://www.ccn.cni.es/index.php/en/docman/documentos-publicos/23-decalogue-spanish-approach- to -cybersecurity-2018 / file
https://www.boe.es/eli/es/rd / 2020/05 / 19/521 / con
https://cybernews.com/security/cybersecurity-in-spain/
https://publicaciones.defensa.gob.es/media/downloadable/files/links/P/D/PDF457.pdf
https://publicaciones.defensa.gob.es/media/downloadable/files/links/m/o/monografia_126.pdf